EMR-ISAC
Emergency Management & Response-Information Sharing & Analysis Center

Highlights:

The U.S. Fire Administration maintains the **Emergency Management and Response – Information Sharing and Analysis Center (EMR-ISAC)**.

For information regarding the EMR-ISAC visit **www.usfa.dhs.gov/emr-isac** or contact the EMR-ISAC office at: **(301) 447-1325 and/or emr-isac@fema.dhs.gov.**

The InfoGram

Volume 15 – Issue 24 *June 11, 2015*

Getting to the Scene Alive: POV Accidents

Every year, many firefighters are killed or injured responding to an accident or fire in their privately owned vehicle (POV). In 2012 and 2013, the U.S. Fire Administration reported four fatalities due to POV accidents each year. Many more accidents happen with firefighter injuries each year, sometimes with civilian injuries or deaths resulting from multivehicle accidents as well.

Volunteer departments rely on POVs for their personnel to respond to the station or directly to incidents. State laws vary on the restrictions and immunity granted to volunteers in POVs as well as whether lights and sirens are either allowed or required. Know your state's laws and regulations. In recent years, firefighters have seen jail time and civil cases resulting in fines over $1 million due to POV accidents resulting in civilian fatalities, and departments were sued as well.

Remember safety starts at the time of the call, and some simple and basic things can mean the difference between life and death:

- Check the map or GPS before leaving for the call, not en route;
- Recognize you are excited. Calm down and don't let it distract your driving;
- Turn off the radio and do not use your cell phone for any purpose while driving;
- Do not assume other drivers notice your lights or siren if you are using them, especially at intersections;
- Do not assume other drivers know you're state laws about responding POVs;
- If your department does not have a policy for POVs (PDF, 104 Kb), create one (PDF, 615 Kb).

Finally, the number one thing you can do for your safety is wear your seatbelt. Of the 2013 POV accident fatalities, none were wearing seatbelts. All firefighters need to wear seatbelts or restraints every time, no matter if they are responding in apparatus or a POV.

(Source: IAFC)

DOJ: Drone Usage Policy for Law Enforcement

Interest in using Unmanned Aerial Systems (UAS), also known as "drones," to assist first responders is on the rise. The use of these devices raise many ques-

tions regarding civil rights and privacy, and while the topic is under consideration by many federal, state, and local agencies, some states have enacted legislation restricting their use by law enforcement.

UAS systems have many uses applicable to law enforcement needs, including missing person searches, active shooter response, traffic accident and crime scene analysis or photography, and other places that would endanger the life of an officer. Finding the balance between uses of UAS and maintaining a good relationship with the community is an important condition for departments to manage.

Last month, the Department of Justice (DOJ) released usage policy guidance toward better internal management of UAS practices. "Domestic Use of Unmanned Aircraft Systems (UAS)" (PDF, 125.5 Kb) is only for law enforcement agencies of the DOJ and is not meant as a regulation or guideline for state, local, or other federal law enforcement agencies. However, it does provide a look at how one agency is handling the new responsibilities of UAS usage.

More information on the legal path first responder agencies can take to use UAS is on the Federal Aviation Administration's website, specifically under the Public Operations section.

(Source: FAA)

Think You Can Identify a Phishing Email?

Every day, companies and people lose money, time, and confidential information due to email phishing scams. RSA found phishing attacks cost $687 million in the first half of 2012 alone. First responder departments and related industries are not immune to this; recently a hospital in Pennsylvania reported it was successfully phished, leading to a compromise of the payroll and benefits system.

Phishing emails are used to steal money, which happens in different ways. In one, a person clicks a link in a phishing email and malicious software gets installed on the computer or mobile device and steals personal information. Another way is for someone to click a link which takes them to an authentic-looking but phony login page (i.e., a bank); when the person enters their login credentials, the information is recorded and used to access the authentic site.

Knowing how much critical and personal information can be stored in networks and servers supporting 9-1-1 call centers, law enforcement agencies, and EMS/medical departments, it is critical your personnel can identify phishing emails. Misspellings, strange punctuation, URLs that don't go where they say they do, and attached .zip files are all clues.

McAfee Security, a technology security company, created the "Email Phishing Awareness Quiz," as seen in this CBS news article. The quiz shows 10 emails seeming to be from legitimate companies and you must decide if each is real or fake. Some of the emails are regarding personal business, some are work-related. Once complete, the site will show you each email and highlight the important things to look for. It also shows how you compare to all quiz-takers, the average score by country, and a link to "7 Tips to Avoid Being Phished."

(Source: Microsoft)

DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local *FBI office* and also the *State or Major Urban Area Fusion Center*.

For information specifically affecting the private sector critical infrastructure contact the **National Infrastructure Coordinating Center** by phone at **202-282-9201**, or by email at **nicc@dhs.gov**.